Network Policy

The College will adopt a uniform set of standards, installation practices, processes, procedures, and operational criteria in the construction, use, and ongoing management of the NCCC network to ensure its secure, effective and efficient use.

The priorities for the NCCC network are safety, security, economy, reliability, and capability. The college's goal is to ensure the integrity and stability of the NCCC network, as well as the efficiency and effectiveness of its construction and operation.

Providing a centrally managed enterprise class institution wide network is most effective and efficient method for achieving NCCC's goals in information transport. This reduces the total cost of ownership to the college and promotes the availability and reliability of its information transport systems for all users. Through central planning and management, the college ensures that the network infrastructure is constructed and operated in an integrated, effective, and efficient manner.

The NCCC network is for the use of the college as a whole and is managed for the benefit of all NCCC users. Therefore, the network is designed and implemented to handle a wide variety of information transport requirements. This network is designed to satisfy most user needs for the transport of information.

General Policy Provisions

- Technology Services will manage and administer the NCCC network utilizing support staff and on-call consulting as needed.
- Use of the NCCC network is governed by the Fair Use Policy for electronic resources.
- All wireless connections to the NCCC network must be made in accordance with, NCCC's Wireless Policy.
- All devices connecting to the NCCC wired network must be centrally registered.
- The configuration and operation of devices connecting to the NCCC network must comply with all applicable NCCC security policies, procedures, and practices,
- Technology Services will determine the security specifications and standards for devices connected to the NCCC data network. Devices connected to the NCCC network will be reviewed on a regular basis for the latest operating system and application security patches applicable to that device as well as the latest anti-virus software. Devices not compliant with IT Security Office standards may be disconnected from the NCCC network.
- All devices/users connecting to the NCCC data network through NCCC's Virtual Private Network (VPN) must use the centrally-provided service and comply with NCCC's VPN Policy**.** Other VPN services are not allowed. The IT Security Office may implement or utilize additional VPN services to enforce confidentiality and integrity of campus data and assets. Devices connecting via a third-party telecommunications provider contracted by the user or a third-party telecommunications provider's dial-up connection may be required to meet certain specifications to utilize the NCCC's VPN service.
- Technology Services will determine the technical specifications, installation practices, standards, and operational criteria for the management and operation of the NCCC network.
- The NCCC data network shall utilize the Internet Engineering Task Force (IETF) open standard suite of protocols collectively known as the Internet Protocol (IP). Vendor proprietary protocols

such as AppleTalk, IPX, or any other proprietary protocols will not be routed over the NCCC data network.

- Units/users may not attempt to implement their own network infrastructure or extend the NCCC network without permission from Technology Services. This includes, but is not limited to, basic network devices such as repeaters, switches, routers, network firewalls, wireless access points, telephone key systems, CATV splitters or virtual extensions using tunneling technologies such as Virtual Private Networking (VPN) hardware and/or software. Units/users may not offer alternative methods of access to the NCCC network, such as modems.
- Devices connecting to the NCCC's data network must use the central Dynamic Host Control Protocol server.
- Devices connecting to the NCCC's data network must use the central Domain Name Service (DNS).
- Division's will be responsible for expenses associated with correction of any unauthorized installation, modification, or resulting repair.
- The college recognizes that certain organizations/departments may require their own information transport networks for academic, research, or other special purposes. However ALL networks of this type utilizing any type of transport media (electrical, photonic or wireless) for any information transport need are considered owned by the college and as such fall under the jurisdiction of the college. Implementation of such networks must be coordinated through NCCC Technology Services.
- The Director of Technology Services can make exceptions to the provisions of this policy in accordance with overall network management and reliability requirements and user needs.

Responsibilities of Technology Services

Information Services responsibilities regarding the NCCC network include but are not limited to:

- monitoring rules, regulations, guidelines, best practices and standards of:

  - Federal Communications Commission (concerning telecommunications)

  - Digital Millennium Copyright Act (DMCA)

  - Building Industry Consulting Service International (BICSI)

  - Telecommunications Industry Association (TIA)

  - Institute of Electrical and Electronics Engineers (IEEE)

  - International Telecommunications Union (ITU)

  - Internet Engineering Task Force (IETF)

  - National Electric Code (NEC)

  - National Electric Safety Code (NESC)

  - Americans with Disabilities Act (ADA)

  - American College and NCCC Telecommunications Association (ACUTA)

- EDUCAUSE

- monitoring the performance of the NCCC network and ensuring its reliability.
- ensuring compliance with the NCCC's privacy practices in relation to network functions. Upon consultation with General Counsel's Office, the CIO may disclose information obtained in network management or review to law enforcement agencies presenting a validly issued subpoena or court order, and to the NCCC administration upon proper authorization through appropriate administrative channels.
- providing systems to ensure device registration and the disconnection of unregistered devices.
- providing systems for communicating network health and planned maintenance downtime to local technical staff.
- providing local technical staff with appropriate tools to address issues affecting devices.

Responsibilities of the Department

- Department directors will be the departmental contact for Networking and Telecommunications Services for ordering new service, requesting changes to existing service, and/or reporting maintenance issues.
- The Department shall notify Information Services of any change in the Department's contact person.

CONSEQUENCES:

Any individual who violates this policy may lose computer or network access privileges and may be subject to disciplinary action as defined in the NCCC fair use policy which may result in a range of sanctions up to and including suspension or dismissal for repeated or serious infractions.